SOPHOS

sophos anti-virus

User manual

DOS/Windows 3.1x

For network and single users

Document date: August 2006

About this manual

This user manual describes Sophos Anti-Virus for DOS/Windows 3.1x. It explains how to

- install Sophos Anti-Virus
- use Sophos Anti-Virus
- disinfect viruses
- configure Sophos Anti-Virus
- update Sophos Anti-Virus.

The manual also provides help in resolving common problems.

Sophos documentation is published on the Sophos CD each month and at www.sophos.com/support/docs/

Technical support

UK (24 hours):	(+44) 1235 559933	support@sophos.com
USA (24 hours):	(+1) 888 767 4679	supportus@sophos.com
Australia (24 hours):	(+61) 2 9409 9111	support@sophos.com.au
France:	(+33) 1 40 90 20 90	support@sophos.fr
Germany (24 hours):	(+49) 6136 91193	support@sophos.de
Italy:	(+39) 02 662810 0	support@sophos.it
Japan (24 hours):	(+81) 45 227 1800	support@sophos.co.jp
Singapore (24 hours):	(+65) 6776 7467	supportasia@sophos.com

A support knowledgebase and virus information are available on the Sophos website www.sophos.com

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.

Contents

Installation

Using Sophos Anti-Virus

Configuration

Updates

Troubleshooting

Appendices

Glossary and index

About Sophos Anti-Virus for DOS/Windows 3.1x

This section contains information about installing and updating Sophos Anti-Virus on DOS/Windows 3.1x.

What is Sophos Anti-Virus?

Sophos Anti-Virus is software that can

- detect viruses
- report virus finds to specified locations
- disinfect viruses.

Sophos Anti-Virus can run on single computers or entire networks.

How is Sophos Anti-Virus installed and updated?

You install Sophos Anti-Virus directly on each DOS/Windows 3.1x workstation or file server from the Sophos CD (section 1). Alternatively, you can make a floppy disk set from the Sophos CD and install from disk.

Sophos Anti-Virus can only detect and disinfect viruses known to Sophos at the time it was released. This means you must update your software regularly to ensure it is capable of recognising the latest viruses. You should update it at the following times:

Every month (section 6)

Every month, Sophos releases a new version of Sophos Anti-Virus on CD and on the website. New versions contain new functionality, as well as the capability to detect the latest viruses. Update any computer on which you installed Sophos Anti-Virus as soon as you receive the Sophos CD.

When there is a new virus that poses a threat to your system (section 7)

When Sophos identifies a new virus, it issues a virus identity file (IDE), a type of file that enables Sophos Anti-Virus to detect that virus. Download IDEs from the Sophos website (www.sophos.com/downloads/ide) and save them to the location specified in section 7.

To receive email alerts about new viruses, register at www.sophos.com/virusinfo/notifications.

What if Sophos Anti-Virus finds a virus?

If a virus is found, find out its name and check its virus analysis on the Sophos website (www.sophos.com/virusinfo/analyses). The analysis should provide disinfection advice. For help with disinfection, contact Sophos technical support.

See also section 3 for general information about disinfection.

Recommended precautions

The book *Computer viruses demystified* (enclosed with your first Sophos CD) describes many common types of viruses and what you can do to avoid being infected by them. If you do not have a copy, a PDF version is available from both the Sophos website and the Sophos CD.

Installation

Installing Sophos Anti-Virus on DOS/Windows 3.1x

1 Installing Sophos Anti-Virus on DOS/Windows 3.1x

This section describes how to install Sophos Anti-Virus on a DOS/Windows 3.1x workstation or file server.

It contains the following information:

- System requirements.
- How to install Sophos Anti-Virus on a workstation to enable on-demand scanning on the workstation.
- How to install Sophos Anti-Virus on a file server to make on-demand scanning available to the DOS workstations connected to the file server.

1.1 System requirement

- MS-DOS version 5.0 or later.
- An Intel 386 machine or better.
- 24 MB of free memory.

1.2 Installing Sophos Anti-Virus on DOS/Windows 3.1x workstations

Before installation you must check that the workstation is free of viruses (section 1.2.1).

You can install Sophos Anti-Virus either on a stand-alone computer (section 1.2.2) or on networked workstations (section 1.2.3).

1.2.1 Checking a workstation is free of viruses

Before installation, it is recommended that you check that the workstation is virus-free. This is done by running Sophos Anti-Virus directly from disk, and requires:

- a write-protected system floppy disk
- the Emergency Sophos Anti-Virus Distribution (ESD) on floppy disk
- a copy of Sophos Anti-Virus on floppy disk.

Utilities for creating the floppy disks are available in the \DISKIMGS folder on the Sophos CD.

❗ The workstation must be booted from a write-protected, virus-free system floppy disk, or some stealth viruses may not be detected.

1. For information on how to create a clean boot disk, see section 3.1.
2. Switch the workstation off and insert the write-protected system floppy disk in drive A:. Switch the power on. Wait until the workstation boots and displays the prompt

   ```
   A:\>
   ```

3. Take the system floppy disk out and insert the first ESD disk. Enter

   ```
   SWEEP *:
   ```

4. Insert Sophos Anti-Virus disks as prompted.

   Sophos Anti-Virus scans the local hard drives.

   If a virus is found, write down its name and check its virus analysis at www.sophos.com/virusinfo/analyses. The analysis should provide instructions for how to disinfect the virus. For assistance, contact Sophos technical support.

1.2.2 Installation on a stand-alone computer

1. Insert the Sophos CD and enter

   ```
   D:\DOS\INSTALL
   ```

   if D: is the CD drive.

   Floppy disk users should insert the first SWEEP for DOS disk and enter A:\INSTALL if A: is the floppy drive.

2. On the **Install** menu, click **New Installation**.
3. Confirm or specify the directory to which Sophos Anti-Virus should be installed.

1.2.3 Installation on networked workstations

1. Copy the contents of the \DOS folder from the Sophos CD to a directory on the server and map this directory to a DOS drive.
2. At a DOS prompt on the workstation, change to that drive and enter

   ```
   DOS\INSTALL
   ```

   Floppy disk users should copy the contents of the SWEEP for DOS disks into a directory on the server and map a drive to this directory. On the workstation, change to this drive and enter INSTALL.

3. On the **Install** menu, click **New Installation**.
4. Confirm or specify the directory to which Sophos Anti-Virus should be installed.

1.3 Installing Sophos Anti-Virus on a file server

On-demand scanning can be made available to all users on the network if you install Sophos Anti-Virus on a file server.

To do this, copy the files from the \DOS folder on the Sophos CD into a publicly accessible read-only area on the server.

If using floppy disks, copy the contents of the SWEEP for DOS disks onto the server.

When installing under NetWare do not mark SWEEP.EXE as execute-only, because Sophos Anti-Virus needs to load overlays when run.

Using Sophos Anti-Virus

Using Sophos Anti-Virus

Disinfection

2 Using Sophos Anti-Virus

This section describes how to use Sophos Anti-Virus to carry out on-demand scans. This is controlled from the command line.

Sophos Anti-Virus can scan floppy disks, hard disks, network drives and memory. It is normal to check the hard disk first and then any suspect floppy disks.

For information on checking compressed files and archives, see section 4.2.

2.1 Secure booting

Before running anti-virus software, ***it is essential to secure boot the computer*** from a write-protected, clean system floppy disk. Failure to do this may result in some stealth viruses not being detected on disk.

1. Switch the computer off. Do not use ‘Ctrl’+ ‘Alt’+ ‘Delete’ because this is intercepted by some viruses.
2. Insert the write-protected system floppy disk into drive A:. Switch the computer on and let it boot from the floppy.

If checking file server drives from a workstation, the secure boot procedure may differ. See section 2.4.

2.2 Checking the hard disk

1. Secure boot the computer (see section 2.1).
2. Change to the SWEEP directory and run the command line version of Sophos Anti-Virus, for example

   ```
   C:
   CD \SWEEP
   SWEEP C:
   ```

   Sophos Anti-Virus scans drive C:.

   To interrupt the scan press ‘Esc’ at any time. Any viruses discovered are listed on the screen.

   To check all hard drives enter

   ```
   SWEEP *:
   ```

2.3 Checking floppy disks

1. Secure boot the computer (see section 2.1).
2. Change to the SWEEP directory and run the command line version of Sophos Anti-Virus, for example

   ```
   C:
   CD \SWEEP
   SWEEP -MU A:
   ```

   Sophos Anti-Virus prompts for the floppy disks to be inserted in drive A:.

2.4 Checking file servers from a workstation

You can use Sophos Anti-Virus to check file server drives from a workstation.

You must establish a network user with read rights before checking. Some viruses infect files at the moment of file open request to DOS. If the user performing the checking has write rights to all files, and such a virus is resident in memory, all files on the server will be infected after scanning the server.

Before running Sophos Anti-Virus, boot up and log into the server securely. The procedure depends on the server platform but must allow a supervisor to log in without executing any DOS programs located on the server.

Scan server drives as follows:

To scan server drives, change to the SWEEP directory and run Sophos Anti-Virus. For example

```
C:
CD \SWEEP
SWEEP <drive1> <drive2> ... <driven>
```

For example, to check drives F: and G:, enter

```
SWEEP F: G:
```

Most networks do not allow examination of the boot sectors of file servers. Furthermore, on most networks, some files (normally .SYS) are not readable and Sophos Anti-Virus reports an error when trying to open them. When scanning a file server drive, by default .SYS files are not scanned. Any other unreadable files can be excluded by quoting them, preceded by the exclusion operator, in the SWEEP.ARE file. For more information see 2.5.

A quick way of finding unreadable files on the file server is to run Sophos Anti-Virus and note the name of any file(s) that could not be opened. There is no loss of security in not checking these, as they contain data and not executable code. They cannot be infected.

2.5 What does Sophos Anti-Virus scan?

By default, Sophos Anti-Virus looks for viruses in the following areas:

- All memory used by programs and viruses.
- All executable files on the specified disk (see latest readme for list of file types defined as executables).
- Logical sector 0 of the specified disk.
- First data sector of the partition (except when running under DOS version 4 or above).
- Physical sector 1 of hard disk devices 80 to 83 Hex (internal hard disks).

Sophos Anti-Virus automatically detects whether files contain macros (and are thus vulnerable to macro virus infection) irrespective of their file extension.

In most cases these default settings are sufficient and there is no need to check any extra items.

To specify additional (or different) areas, or file types, use the command line or create a file called SWEEP.ARE. The syntax for describing areas to be scanned in SWEEP.ARE is described in section 4.8.

To display items checked by Sophos Anti-Virus, use the -DA command line option:

```
SWEEP -DA
```

2.6 What if Sophos Anti-Virus reports a virus or virus fragment?

If Sophos Anti-Virus reports a virus or virus fragment, it has almost certainly discovered a virus. However, there is a small chance that the virus has been matched by a legitimate, virus-free program. If in doubt, contact Sophos technical support for advice.

The screen output looks like this:

```
SWEEP virus detection utility
Version 3.36
Copyright (c) 1989,2000 Sophos Plc, Oxford, England

System time 11:35:30, System date 08 August 2000
Virus library date 07 August 2000 (53396 viruses)

Quick Sweeping
Press Esc to quit

>>> Virus 'Form' found in abs sector 1, drive 00 (floppy disk)
    head 0, cyl 0
0 files swept in 0 minutes and 4 seconds.
1 virus was discovered.
0 files out of 1 were infected.

For advice email support@sophos.com or telephone +44 1235 559933.
```

A virus is reported in the line which starts with '>>>' followed by either 'Virus' or 'Virus fragment'. In the above example no files were infected because Form is a boot sector virus.

For information on dealing with viruses, see section 3.

3 Disinfection

Sophos Anti-Virus's automatic disinfection facilities, or DOS commands, can deal with many virus attacks:

- Infected boot sectors can be disinfected (in some cases) or neutralised.
- Infected files can be deleted.
- Infected documents can be disinfected.

The sections below explain how to prepare for disinfection and how to deal with each kind of infected item.

❗ Sophos Anti-Virus does not perform disinfection if it detects a virus active in memory, since severe data corruption could result. It is always advisable to reboot from a clean disk, as recommended in the sections below.

3.1 Creating a clean DOS boot disk

A clean boot disk (i.e. an uninfected write-protected system floppy disk) is an essential part of the virus recovery procedure.

To create a bootable system floppy disk do the following:

1. At a DOS prompt on the computer enter:

```
FORMAT A: /S
```

2. Copy HIMEM.SYS, FDISK.EXE, SYS.COM, DEBUG.EXE, SCANDISK.EXE (or CHKDSK.EXE for MS-DOS 5 and before), EDIT.COM and FORMAT.COM onto the disk. HIMEM.SYS is an Extended Memory (XMS) driver which enables Sophos Anti-Virus to use all the computer's memory thereby improving performance.

3. Create a CONFIG.SYS file with the following lines:

```
DEVICE=A:\HIMEM.SYS
DEVICE=A:\EMM386.EXE
DOS=HIGH, UMB
FILES=20
BUFFERS=4
```

4. Create an AUTOEXEC.BAT with the following lines:

   ```
   SET TEMP=C:\
   SET TMP=C:\
   ```

   If you are using DRVSPACE, DBLSPACE, Stacker, hard disk overlay managers or similar software you need additional drivers to access the hard disk.

   Make the floppy disk write-protected (to ensure that it cannot become infected with a virus), and label it with the operating system for which it was created.

   If a computer becomes infected, use the clean boot disk to boot the computer. This ensures that various items on the computer can be examined through a clean operating system.

3.2 Disinfection of boot sectors

Sophos Anti-Virus can eliminate boot sector viruses on the hard disk or on floppy disk.

3.2.1 Disinfecting boot sectors on the hard disk

Hard disks with infected boot sectors can either be disinfected or have their boot sectors replaced with clean ones.

Disinfection

This is the preferred approach. Before attempting this, it is advisable to backup any important data contained on the hard disk.

Boot the PC with a clean boot disk. Use Sophos Anti-Virus to disinfect the virus with the command

```
SWEEP -DIB C:
```

Replacing the boot sector

Alternatively, the boot sector can in many cases be overwritten with a clean one.

1. Boot the PC with a clean boot disk, and check that the contents of the infected drive are visible (e.g. with DIR).

2. If the directory listing is okay, overwrite the master boot sector with the command

   ```
   FDISK /MBR
   ```

   or the DOS boot sector with

   ```
   SYS C:
   ```

   If you use the SYS command to overwrite a DOS boot sector virus, it is essential that the clean boot disk is the same version of DOS as the infected computer.

   Also, if the infected computer is not running DOS, the DOS-specific command SYS should not be used.

If the contents of the hard disk are not visible after a clean boot, contact Sophos technical support for advice. Some boot sector viruses require additional action for full recovery.

3.2.2 Disinfecting boot sectors on floppy disk

Floppy disks with infected boot sectors can either be disinfected or reformatted.

Disinfection

Boot the computer with a clean boot disk. Then disinfect the virus using

```
SWEEP A: -DIB
```

To scan and disinfect a number of floppy disks, use

```
SWEEP A: -DIB -MU
```

Sophos Anti-Virus prompts for each disk to be inserted in turn. It is important to check ***all*** floppy disks that have been used in infected computers.

Reformatting

Boot the computer with a clean boot disk, copy the valuable data from the infected disk to a clean destination (it is safe to copy files if the computer has been booted from a clean boot disk), and reformat the disk using

```
FORMAT A:
```

where the disk is in drive A:.

3.3 Disinfection of infected executable files

Attempting to disinfect executables is not recommended as it is impossible to ensure that executables are properly restored after disinfection. Restored files may be unstable, putting valuable data at risk.

However, as a short-term measure, use the command

```
SWEEP -DIPE
```

to disinfect any infected Windows program files (PE executables).

You should then boot the computer with a clean boot disk. Locate all the infected executables, delete them, and restore clean versions from the original installation disks, from a clean computer, or from sound backups.

3.4 Disinfection of infected documents

Sophos Anti-Virus can automatically disinfect documents infected with macro viruses.

It is not necessary to reboot from a clean system disk, but it is important to ensure that the application that created the document is not open when disinfection is attempted. Use the command

```
SWEEP -DID
```

3.5 Recovering from virus side-effects

Recovery from virus side-effects depends on the virus. In the case of innocuous viruses such as *Cascade,* recovery from side-effects is not necessary, while in the case of a virus such as *Michelangelo*, recovery usually involves the restoration of a complete hard disk from the most recent backups.

Some viruses, such as *WM/Wazzu* gradually make minor changes to users' data. This sort of corruption (e.g. the removal of the word 'not' from a sentence in a Word file) can be very hard to detect and highly undesirable.

The most important thing when recovering from virus side-effects is the existence of sound backups. Original executables should be kept on write-protected disks so that any infected or disinfected programs can easily be replaced by the original clean versions.

Sometimes data can be recovered from disks damaged by a virus. Sophos can also supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice.

Configuration

Configuring Sophos Anti-Virus

Command line options

4 Configuring Sophos Anti-Virus

This chapter describes

- how to specify what Sophos Anti-Virus will scan (section 4.1)
- how to scan compressed files (section 4.2)
- full and quick scanning (section 4.3)
- how to scan with new patterns (section 4.4)
- how to customise the virus-found report (section 4.5)
- how to run Sophos Anti-Virus from batch files (section 4.6)
- how to scan dynamically compressed drives (section 4.7)
- how to specify what Sophos Anti-Virus will scan with SWEEP.ARE (section 4.8).

4.1 Specifying what Sophos Anti-Virus will scan

The files or areas to be scanned can be specified from the command line (as described in this section), or in an area file (see section 4.8).

4.1.1 Specifying drives to be scanned

To scan the current drive only, do not specify any drives in the command line. Use the command

```
SWEEP
```

To scan one or more drives**,** specify them in the command line, e.g. to scan drives C: and D:, use

```
SWEEP C: D:
```

If one or more drives are specified, Sophos Anti-Virus will ***not*** scan the current drive in addition to these.

To scan all hard drives, use the '*:' option:

```
SWEEP *:
```

This is useful when the number of hard drives is unknown (e.g. when invoking Sophos Anti-Virus from a file server to scan all workstation hard drives).

4.1.2 Specifying files to be scanned

Items to be scanned can be specified in the command line. For example, to scan the file ISVIRUS.BIN type

```
SWEEP ISVIRUS.BIN
```

Make sure that any symbols used do not conflict with the MS-DOS meaning. For example, do not use the recursion symbol '>' in the command line, because it means redirection in MS-DOS.

If one or more items are specified in the command line, Sophos Anti-Virus will scan only these items.

4.2 Scanning compressed files

The approach depends on the kind of compressed files encountered:

- **Archive files**, or 'statically compressed' files, such as those compressed with PKZIP, consist of one or more files that have been compressed and combined to form a single file.
- **Dynamically compressed files**, such as those compressed with PKLITE, LZEXE etc., consist of compressed data and a program to compress that data. The data can be infected before compression, while the decompression program can be infected at any time after compression.

Some utilities, such as Doublespace, allow compression of whole drives. Section 4.7 explains how to deal with these.

Archive files

Sophos Anti-Virus can scan inside archive files if it is run with the -ARCHIVE option. To display the archive types that are scanned, enter

```
SWEEP -VV
```

You can also enable or disable scanning of particular archive types. See section 5.2 for full details.

Dynamically compressed files

By default, Sophos Anti-Virus will scan files compressed with PKLITE, LZEXE and Diet.

4.3 Full and quick scanning

By default, Sophos Anti-Virus carries out a quick scan, which scans only those parts of files likely to contain viruses.

If a full scan is specified (using the -F option), the entire file contents are scanned. For example

```
SWEEP -F B:
```

performs a full scan of drive B:.

4.4 Scanning with new patterns

The range of patterns scanned by Sophos Anti-Virus can be extended by creating a file called SWEEP.PAT containing the patterns in the following format:

```
Name Hex1 Hex2 ... Hexn ; Comments
```

where

- `Name` is the pattern name (no spaces allowed)
- `Hex1` etc. are pattern bytes in hexadecimal, 2 hexadecimal digits per byte, most significant nibble first
- `Comments` are any comments after the '`;`'

Pattern bytes can be separated by spaces or tabs. A name can contain up to 15 characters and a pattern can be up to 24 bytes long.

If the line starts with a space or a tab, the pattern will have the name 'Noname n' where n is a number from 0 upwards.

For example, SWEEP.PAT may contain

```
ABC_Virus 26 83 88 9c 9f f9 f0 23
HAL_Virus ABCDEF0123456789 ; comment
```

SWEEP.PAT must reside in the current drive and subdirectory when Sophos Anti-Virus is run. For example, if the current drive and directory is C:\PROGS and drive A: is being scanned using the command

```
SWEEP A:
```

SWEEP.PAT must reside in the directory C:\PROGS.

Sophos Anti-Virus only looks for patterns when it runs a full scan (see section 4.3). Thus, the -F option must be used.

4.5 Customising the 'Viruses Found' report

Sophos Anti-Virus displays a warning if it discovers one or more viruses. This warning can be customised, for example

```
Contact IT Immediately on Ext 4321!
```

by adding the appropriate text to the file SWEEP.MSG in the current directory.

To specify a different filename use the -FM command line option.

4.6 Running Sophos Anti-Virus from batch files

Sophos Anti-Virus returns error codes that can be tested by using the IF ERRORLEVEL command in batch files. This enables automatic action to be taken if Sophos Anti-Virus discovers an abnormal condition. Sophos Anti-Virus returns

- 0 if no errors are encountered and no viruses are found
- 1 if the user interrupts the execution by pressing 'Esc'
- 2 if some error preventing further execution is discovered
- 3 if viruses or virus fragments are discovered.

These return values can be tested by using the IF ERRORLEVEL command. For example

```
@ECHO OFF
SWEEP -NK
IF ERRORLEVEL 3 GOTO FISHY
IF ERRORLEVEL 1 GOTO SOMEERR
ECHO No problems
GOTO END
:SOMEERR
ECHO Some error has occurred
GOTO END
:FISHY
ECHO Something has been discovered
:END
```

This batch file will print

```
Something has been discovered
```

if Sophos Anti-Virus discovers a virus,

```
Some error has occurred
```

in the event of an error, or

```
No problems
```

if nothing is discovered. The -NK option tells Sophos Anti-Virus not to pause for a keystroke if it discovers a virus.

Remember that IF ERRORLEVEL means if level is greater or equal to the specified value.

Extended error codes

A different set of error codes is returned if Sophos Anti-Virus is run with the -EEC command line option.

- 0 If no errors are encountered and no viruses are found.
- 8 If survivable errors have occurred.
- 16 If password-protected files have been found (they are not scanned).
- 20 If viruses have been found and disinfected.
- 21 If infected files have been found and deleted.
- 22 If infected files have been found but deletion failed.
- 24 If viruses have been found and not disinfected.
- 28 If viruses have been found in memory.
- 32 If there has been an integrity check failure.
- 36 If unsurvivable errors have occurred.
- 40 If execution has been interrupted.

4.7 Scanning dynamically compressed drives

Some utilities allow transparent dynamic compression of whole drives. These will not be accessible if the user boots up from a standard system floppy disk, as is usually the case before using Sophos Anti-Virus.

This section explains how to create system disks that make it possible to access and scan drives compressed with Doublespace (supplied with MS-DOS 6), Stacker and Superstor.

4.7.1 Drives compressed with Doublespace (MS-DOS 6)

To create a bootable floppy disk use

```
FORMAT A: /S
```

while Doublepace compression is active.

As well as the two hidden system files (IBMBIO.SYS and IBMSYS.SYS or similar), the operating system automatically creates a third file DBLSPACE.BIN which contains the compression code.

After booting from such a system floppy disk, the compressed drive can be accessed and scanned for viruses as normal.

4.7.2 Drives compressed with Stacker

Stacker uses a device driver which is loaded through CONFIG.SYS. So the procedure is as follows:

1. Format a bootable DOS system floppy disk using

   ```
   FORMAT A: /S
   ```

2. Copy the file C:\STACKER\STACKER.COM to the floppy disk.
3. Copy the file C:\STACKER\SSWAP.COM to the floppy disk.
4. The file CONFIG.SYS on the hard disk should have two lines which refer to STACKER and look like:

   ```
   DEVICE=C:\STACKER\STACKER.COM C:\STACKVOL.DSK
   DEVICE=C:\STACKER\SSWAP.COM C:\STACKVOL.DSK /SYNC
   ```

   These lines should be copied into CONFIG.SYS on the floppy disk, but the references to C:\STACKER should be replaced with A:\. The above file would read:

   ```
   DEVICE=A:\STACKER.COM C:\STACKVOL.DSK
   DEVICE=A:\SSWAP.COM C:\STACKVOL.DSK /SYNC
   ```

It is important that no other parts of those lines are changed.

After booting from such a system disk, the compressed drive can be accessed and scanned for viruses as normal.

4.7.3 Drives compressed with Superstor

1. Create a bootable floppy disk using the command

   ```
   FORMAT A: /S
   ```

2. The files SSTORDRV.SYS and DEVSWAP.COM should be copied to the floppy. The CONFIG.SYS file on the floppy should contain

   ```
   DEVICE=A:\SSTORDRV.SYS
   DEVICE=A:\DEVSWAP.COM
   FILES=20
   BUFFERS=20
   ```

   After booting from such a system disk, the compressed drive can be accessed and scanned for viruses as normal.

4.8 Specifying what Sophos Anti-Virus will scan with SWEEP.ARE

Items to be scanned can be specified in an area file (SWEEP.ARE).

This must reside in the current drive and subdirectory when you run Sophos Anti-Virus. For example, if the current drive and directory is C:\PROGS, SWEEP.ARE must reside on the C: drive in the directory C:\PROGS.

SWEEP.ARE can contain a list of files, sectors and memory regions to be scanned. This file can be edited as required. The syntax for describing areas to be scanned is given in the following sections.

Example of a SWEEP.ARE file

```
D:|0
D:\>*.EXE
D:\>*.OVL
+81 0 0 1
```

This will scan the DOS boot sector on drive D:, all EXE and OVL files on drive D: and physical sector 1 on the second hard disk.

The | symbol is the DOS ‘pipe’ operator and is not the same as 1 (digit) or l (character).

The default drive in the command line can be overridden by using the -AD option. For example, to scan drive A: while Sophos Anti-Virus is on drive C: you would type

```
SWEEP -AD=A:
```

If the drive is not specified, the default drive will be used. For example, if SWEEP.ARE contains

```
*.*
D:|0
```

and the command

```
SWEEP -AD=A:
```

is issued, then Sophos Anti-Virus would scan

```
A:*.*
D:|0
```

in addition to the standard areas on drive A:.

4.8.1 Specifying files to be scanned with SWEEP.ARE

Particular file types and areas can be specified in SWEEP.ARE using the normal DOS descriptions. For example

```
C:\*.ABC
```

will make Sophos Anti-Virus examine all files with extension .ABC in the root directory of drive C:.

The recursion operator '>' can be used to specify that all subdirectories, as well as the specified directory, should be searched. For example, if the entry

```
C:*.ABC
```

is specified, and the current directory of drive C: contains two subdirectories, ***only the current directory*** will be searched for .ABC files.

On the other hand, if the entry

```
C:>*.ABC
```

is specified, not only the current directory, but also both subdirectories will be searched for .ABC files. Similarly, if the entry

```
C:\MYAREA\MYFILES\>*.ABC
```

is specified, the search will cover the directory C:\MYAREA\MYFILES and all its subdirectories.

See also the -REC command line option.

To scan all executables

To scan all executable files, specify

```
C:"All executables"
```

Scanning is about 30% faster than when each group is specified individually. The drive specification ('C:' in above example) is optional.

Excluding files

Certain files or directories can be excluded from scanning, by preceding the description with the '<' exclusion operator. For example

```
C:>*.EXE
<C:\DONOT.EXE ; will not be examined
```

will recursively search all EXE files except DONOT.EXE in the root directory.

If the name of a file is specified ***without a path***, all files or directories with that name will be excluded. For example

```
<ALL.EXE ; will not be examined
```

will not examine the file ALL.EXE in any subdirectory in which it is found, e.g. files C:\EXE\ALL.EXE, C:\FIX\DEVELOP\ALL.EXE etc.

Excluding a directory excludes all files and subdirectories of that directory.

The drive, path and filename of the included and excluded items must be ***identical***. For example, if the user specifies

```
C:\>*.COM
```

to be examined and excludes

```
<\WS.COM
```

the file 'C:\WS.COM' will still be examined. To exclude it, specify

```
<C:\WS.COM
```

Likewise, if the specification is

```
\>*.EXE
```

and the current drive is C:, specifying

```
<C:\NU.EXE
```

means that Sophos Anti-Virus will still scan 'NU.EXE' in the root directory. To exclude it, specify

```
<\NU.EXE
```

Wildcard characters * and ? can be used with the exclusion operator.

Any exclusion descriptors that contain the '\' symbol and do not specify a drive will have the drive specified in the -AD option. For example, if SWEEP.ARE contains

```
<\NU.EXE
```

and Sophos Anti-Virus is started with the option

```
SWEEP -AD=C:
```

the file which will be excluded will be C:\NU.EXE. This is equivalent to entering

```
<C:\NU.EXE
```

in the SWEEP.ARE file.

4.8.2 Specifying disk sectors to be scanned with SWEEP.ARE

At a lower level than the file structure, disks are organised into sectors. The most important of these are the master boot sector and the DOS boot sector, as they contain executable program code which many viruses attack. A floppy disk has only a DOS boot sector.

There are logical sectors and absolute sectors.

A logical sector number refers to the position of the sector within a particular drive or partition. This is useful when referring to the DOS boot sector, which is logical sector 0 of the partition.

The absolute sector number describes the physical position of the cylinder, head and sector on the specified device. While more complex than a logical sector number, it allows any sector on the disk to be specified. This is important for scanning the master boot sector, found at cylinder 0, head 0, sector 1. On hard disks this sector is not accessible using a logical sector number. On floppy disks, the absolute sector at cylinder 0, head 0, sector 1 and logical sector 0 are the same physical sector.

Logical Sectors

To specify a particular logical sector or set of sectors, use the '|' symbol (the DOS pipe operator). You can also specify a byte or group of bytes to be scanned in each sector (e.g. if the sector contains variable information). The format of the specification is

```
drive | ssector esector sbyte ebyte
```

where

- `drive` is the drive letter, e.g. C: (optional)
- `ssector` is the first logical sector to be scanned
- `esector` is the last logical sector to be scanned (optional)
- `sbyte` is the first byte to be scanned (optional)
- `ebyte` is the last byte to be scanned (optional).

All values must be in ***decimal*** format. For example

```
C:|0
```

specifies that the whole of logical sector 0 on drive C: should be scanned, whereas

```
C:|0 10
```

specifies that logical sectors 0 to 10 inclusive should be scanned.

Specifying ‘F’ as ssector will scan the first data sector of the drive. For example

```
C:|F
```

will scan the first data sector of the drive C:.

This sector needs to be scanned only on DOS versions prior to version 5.0, due to the way that the system files are loaded during the boot process.

In addition, the ‘`|*`’ specification can be used:

```
|*
```

This scans all sectors within the current logical disk ***and should be used with care***; it may find virus fragments in deleted files and may cause false positives.

Absolute Sectors

To specify an absolute sector, use the ‘`+`’ symbol followed by the drive number, the cylinder (or ‘track’) number, the head (or ‘side’) number and the sector number within that cylinder. The first floppy disk drive in the system is number 0, the second is number 1, and so on. The first physical hard disk drive is number 80, the second is number 81 and so on.

The format of the specification is

```
+drive cylinder head sector
```

where

- `drive` is the disk drive number
- `cylinder` is the cylinder number
- `head` is the head number
- `sector` is the sector number.

All values must be in ***hexadecimal*** format. For example

```
+80 0 0 1
```

specifies that sector 1 of cylinder 0, head 0 on the first fixed disk (usually drive C:) should be scanned.

To scan master boot sectors on disks 80 to 83 Hex, specify

```
"All master boot sectors"
```

If a particular disk is not present, no error message is produced.

4.8.3 Specifying memory ranges for scanning

Intelligent memory scanning (i.e. only memory used by programs and viruses) is enabled by default, but can be explicitly specified in SWEEP.ARE by

```
"All memory"
```

or by using the -ME command line option:

```
SWEEP -ME
```

Intelligent memory scanning is less prone to false positives than scanning all 640KB of base memory.

Other areas of memory can be scanned for the presence of virus fragments. To specify memory ranges, use the ‘[‘ symbol. The format of the specification is

```
[segment:sbyte ebyte]
```

where

- `segment` is the memory segment (assumed to be 0000 if not specified)
- `sbyte` is the address of the first byte to be scanned (optional)
- `ebyte` is the address of the last byte to be scanned (optional).

Note that all values are in ***hexadecimal*** format.

For example

```
[0000:0000 00FF]
```

specifies that bytes 0000 to 00FF hex within segment 0000 should be scanned.

In addition, the following specification can be used:

```
[*]
```

This scans all 640KB of base memory. The [*] option can be specified in the command line. For example

```
SWEEP [*]
```

Scanning all 640KB of base memory can cause false positives, especially when more than one anti-virus product is used and one of these products does not encrypt (or scramble) virus fragments held in memory. A false positive may also be reported during an immediate scan run after a virus has been successfully disinfected. The remnant of the virus may still be present in system buffers and will be flagged if the whole of base memory is scanned. This does not ***necessarily*** mean that the virus is active in memory.

5 Command line options

This section describes the Sophos Anti-Virus command line options.

5.1 Command line format

Sophos Anti-Virus accepts certain command line options to control and/or automate the scanning process (sometimes called a SWEEP). These options are described in the following subsections, or can be listed using

```
SWEEP -?
```

The command format is

```
SWEEP drive1 ... driven file1 ... filen q1 ... qn
```

where

- `drive1 to driven` are the drives which will be checked (A:, B:, C: etc.) and '*:' denotes all hard drives
- `file1 to filen` are descriptors of files checked
- `q1 to qn` are command line options (all beginning with either a hyphen '-' or a slash '/')

For example

```
SWEEP C: -F
```

will scan hard drive C: in full mode (-F).

5.2 Command line options

@file Command line options from an external file

Sophos Anti-Virus can obtain its command line options from an external text file. For example, if a file called EXAMPLE.TXT contained

```
*:
```

entering

```
SWEEP @EXAMPLE.TXT
```

would scan all hard drives on the computer.

This feature is normally used to avoid exceeding command line length limitations.

-? or -H or -HELP

Causes Sophos Anti-Virus to display all command line options along with a short description of their function.

-A Append report

By default, any security report written to a file by Sophos Anti-Virus is overwritten by a subsequent report written to a file of the same name. Specifying the -A option in the command line, for example

```
SWEEP -A -P=FOO.REP
```

directs Sophos Anti-Virus to append the new report to the old file FOO.REP, rather than overwriting the old report.

If this is used in an automatic process, this file should be purged from time to time to stop it taking up increasing disk space, especially if the -NS command line option is used.

-AD=<drive> Area file default

Any files or areas listed in the SWEEP.ARE file are assumed to be in the current drive, unless they have an explicitly stated drive. For example

```
SWEEP -AD=D:
```

would assume that all areas refer to drive D:.

-AF=<filename> Area file

The default area file is called SWEEP.ARE. The -AF option can be used to specify a different name.

See also section 4.8.

-ALL Scan all files

In order to scan all files on a disk, instead of just the executable files, specify -ALL. This is equivalent to creating a SWEEP.ARE file which contains

```
\>*.*
```

It thus specifies a recursive search of all files (rather than just executable files) from the root directory of the current drive. For example

```
SWEEP A: -ALL
```

checks all files on drive A:.

This is a slow process which can cause false positives. It can also cause problems on file servers when Sophos Anti-Virus tries to open files already in use.

-ARCHIVE Scan inside archive files

This option enables Sophos Anti-Virus to scan inside archive and self-extracting archive files. File types scanned include: ZIP, GZIP, RAR, ARJ, CMZ, TAR, UUE and Lha. It does not include cabinet files, see -CAB.

You can also disable scanning of particular archive types. For example

```
-ARCHIVE -NZIP
-ARCHIVE -NRAR
```

See also -SFX.

-ARJ Scan inside .arj files

Enables Sophos Anti-Virus to scan inside .arj files.

-AS Scan standard areas

If an area to be scanned is specified in the command line, Sophos Anti-Virus will not scan standard areas such as the master boot sector. With -AS , standard areas are also scanned.

For example

```
SWEEP SUSPFILE.EXE -AS
```

will scan SUSPFILE.EXE as well as the standard areas.

-CAB Check inside cabinet files

Enables Sophos Anti-Virus to check inside Microsoft cabinet files.

-CDR Scan CD boot image

To scan the boot image of a CD, use the -CDR option. For example

```
SWEEP -CDR D:
```

scans all executables, logical sector 0 and the boot image (if any) of drive D:. The boot image contains the boot sector and some files. If Sophos Anti-Virus finds a boot image, it scans the boot sector of that image for boot sector viruses.

To scan all executables in the boot image for program viruses, use the -LOOPBACK option. For example

```
SWEEP -CDR -LOOPBACK D:
```

scans all executables, logical sector 0 and the boot image (if any) of drive D:. If Sophos Anti-Virus finds a boot image, it scans the boot sector of that image for boot sector viruses and all executables in that image for program viruses.

-CI Check integrity

Causes Sophos Anti-Virus to perform an extra-stringent integrity check of SWEEP.EXE before executing (this is in addition to the standard integrity check). A change in the contents of SWEEP.EXE may indicate the presence of a virus or some other form of data corruption. Note that if a stealth virus is present in memory, as well as on SWEEP.EXE, the change in the integrity of SWEEP.EXE may not be detected.

-CMZ Scan inside .Z files

Enables Sophos Anti-Virus to scan inside .Z files.

-D=<day|percentage> Execute only on day or percentage of times

Sophos Anti-Virus may be placed in the AUTOEXEC.BAT file; however it may not be desirable to perform the system check every time the computer is switched on. -D enables you to specify either the probability with which Sophos Anti-Virus will scan the system, or the day of the week on which it will scan the system. For example

```
SWEEP -D=MONDAY
```

will only run Sophos Anti-Virus when invoked on a Monday. The day of the week can be abbreviated to a minimum of two letters (e.g. MO for Monday, TU for Tuesday).

Alternatively

```
SWEEP -D=20
```

will make Sophos Anti-Virus check the system on average 20 out of every 100 times that it is invoked. The number specified must be an integer between 0 and 100.

See also -DE.

-DA Display areas

Lists all areas to be scanned by Sophos Anti-Virus, but does not actually scan them.

-DE Daily execution

Checks whether Sophos Anti-Virus has already been executed that day and if it has, will not allow it to be executed again.

The file SWEEP.DAY is created on the current drive and in the current directory.

A different file can be specified by including '=filename' after -DE. For example

```
SWEEP -DE=sweep.da1
```

-DI Disinfect

Enables Sophos Anti-Virus to perform automatic disinfection of some boot sector, macro and Windows program viruses. See section 3.

-DIB Disinfect boot sectors

As -DI, but instructs Sophos Anti-Virus to disinfect boot sector viruses it is capable of disinfecting.

-DID Disinfect macro viruses

As -DI, but instructs Sophos Anti-Virus to disinfect documents it is capable of disinfecting.

-DIPE Disinfect Windows program files

As -DI, but instructs Sophos Anti-Virus to disinfect Windows program file (PE executable) viruses it is capable of disinfecting.

-DL Display library

Displays the names of all viruses Sophos Anti-Virus is capable of detecting, but does not actually run a scan.

-DN Display names of files as they are scanned

Displays the names of files being scanned. The display consists of the time followed by the item being scanned.

-EF=<filename|path> Exclude file(s)

Directs Sophos Anti-Virus to exclude the file(s) specified from scanning. You can use the backslash character \ in the <filename|path> expression to indicate you are specifying a path. Otherwise, the expression refers to one or more files. You can also use the wildcard character ? to refer to any single character, and the wildcard character * to refer to any number of characters (including zero). For example

```
SWEEP -EF=PIC*.BMP
```

directs Sophos Anti-Virus to exclude any .bmp file whose name begins PIC and which exists in any directory.

```
SWEEP -EF=\PIC?.BMP
```

directs Sophos Anti-Virus to exclude any .bmp file whose four-character name begins PIC and which exists in the root directory.

```
SWEEP -EF=*\PIC\*
```

directs Sophos Anti-Virus to exclude any files in any directory called PIC or to exclude any subdirectory thereof.

```
SWEEP -EF=*P*
```

directs Sophos Anti-Virus to exclude any file whose name contains the letter P and which exists in any directory.

-EX=<extensions> Executable extensions

Enables you to specify the file extensions that Sophos Anti-Virus treats as executables.

For the default list, see the latest readme.

-F Full scan

By default, Sophos Anti-Virus carries out a quick scan, which scans only those parts of files likely to contain viruses. -F specifies a full scan, causing the entire file contents to be scanned. For example

```
SWEEP -F B:
```

performs a full scan of drive B:. A full scan is ***significantly*** slower than a quick scan.

-FM=<file> Specify message file

Sophos Anti-Virus outputs the contents of the file specified with -FM=MESSAGEFILE to the screen if it discovers a virus and MESSAGEFILE exists. This facility is used to customise virus recovery procedures. The default file name of MESSAGEFILE is SWEEP.MSG. For example

```
SWEEP -FM=MY_MSG.TXT
```

specifies the file MY_MSG.TXT.

-GZIP Scan inside .gz files

Enables Sophos Anti-Virus to scan inside .gz files.

-IDE Use alternative directory for virus identity files (IDEs)

This option enables you to specify either an alternative directory for IDEs or a specific IDE.

If you type

```
SWEEP -IDE
```

without specifying a directory or IDE, Sophos Anti-Virus reads IDEs from the root directory of drive A: instead of the default directory (C:\SWEEP).

If you specify a directory, Sophos Anti-Virus reads IDEs from the specified directory instead of the default directory. You may specify the drive. For example

```
SWEEP -IDE=C:\SAVIDES
```

directs Sophos Anti-Virus to read IDEs from the C:\SAVIDES directory instead of the default directory.

If you specify an IDE, Sophos Anti-Virus reads only the IDE instead of those in the default directory. You may specify the drive and path. For example

```
SWEEP -IDE=C:\SAVIDES\IGLOO15.IDE
```

directs Sophos Anti-Virus to read ***only*** the IGLOO15 IDE from the C:\SAVIDES directory instead of the IDEs in the default directory.

-Lang Set display and report language

Sets the language of text displayed in the DOS prompt used to control Sophos Anti-Virus.

-ME Check memory

By default, Sophos Anti-Virus scans memory for viruses. This option is only necessary if memory scanning has been switched off using -NM.

-MU Check multiple disks

Enables you to check a succession of floppy disks in a drive without reloading SWEEP.EXE every time.

For example, to check multiple floppy disks in drive A: type

```
SWEEP -MU A:
```

When prompted, insert a disk in drive A: and press any key to start the scan. Once that disk has been scanned, insert another disk into drive A: when prompted, and press any key to start the next scan.

This will continue until ‘Esc’ is pressed to interrupt scanning.

-NAF Do not read file with areas to be checked

By default Sophos Anti-Virus tries to open the area file SWEEP.ARE and read from it the names of any areas to be scanned. Use this option if Sophos Anti-Virus is not required to check the areas defined in the area file.

-NAS Do not check standard areas

By default, Sophos Anti-Virus scans standard areas defined at compile time. Use this command line option to prevent these areas from being scanned (e.g. if the areas to be scanned have been defined in SWEEP.ARE).

SWEEP.ARE must reside on the current drive and in the current subdirectory.

-NB No bell

Disables the bell that Sophos Anti-Virus by default sounds on discovering a virus or virus fragment.

-NCI Do not check identities

Sophos Anti-Virus normally searches for identities. This option disables the search.

-NCLEAN Scan graphic files

Sophos Anti-Virus recognises graphic file formats that don't pose a viral threat (e.g. GIF, TIFF and JPEG). Therefore, by default it doesn't scan them. However, to enable Sophos Anti-Virus to scan them, use this command line option.

-NDI Do not disinfect infected items

Sophos Anti-Virus only tries to disinfect infected items if the -DI command line option is specified. -NDI is only necessary if a -DI has been used (e.g. in a batch file or within a file specified by @file).

-NE Do not use the emulator

Sophos Anti-Virus finds various polymorphic viruses by emulating the environment in which the virus code would normally execute, making the virus decrypt and reveal itself. -NE speeds up Sophos Anti-Virus, but may lead to some polymorphic viruses not being found.

-NI No interrupting

Execution of Sophos Anti-Virus can normally be interrupted by pressing 'Esc' or 'Ctrl' + 'C'. When -NI is used, execution cannot be interrupted.

-NK No key to continue

If Sophos Anti-Virus discovers one or more viruses or virus fragments, it pauses at the end of the security report and asks for a key to be pressed before continuing. To skip this, use -NK.

-NM No memory check

By default, Sophos Anti-Virus performs an intelligent memory check. When -NM is used, memory is not checked.

-NOC No confirmation before virus removal

Prevents Sophos Anti-Virus from asking for confirmation before disinfecting a document, deleting an infected file or disabling an infected boot sector. This option has no effect unless -REMOVE is also specified. Use this option with care.

For example

```
SWEEP -REMOVE -NOC
```

-NP Do not display full pathname

If Sophos Anti-Virus is set to display the names of the areas scanned, it normally displays the full path of the files it scans (see the -NS option). When -NP is used, Sophos Anti-Virus records names instead of areas.

For example, the output after entering

```
SWEEP -NS -NP
```

might include

```
Examining area 4: C:"All executables"
  CONFIG.SYS
  MSDOS.SYS
  COMMAND.COM
  IO.SYS
```

-NS Not silent

By default, Sophos Anti-Virus does not display the names of areas during scanning. -NS causes the name of each area to be displayed as it is scanned.

For example, the output after entering

```
SWEEP -NS
```

might include

```
Examining area 4: C:"All executables"
  C:\CONFIG.SYS
  C:\MSDOS.SYS
  C:\COMMAND.COM
  C:\IO.SYS
```

-NS also affects the information that is placed in the security report, if such a report is to be created.

-NSC Do not scan compressed files

By default, Sophos Anti-Virus scans compressed files. -NSC switches this off.

-NTW No Temp Warning

Sophos Anti-Virus performs a check to ensure that either the TEMP or TMP environment variables point to a valid path in which Sophos Anti-Virus can create temporary files. A warning is issued if this check fails. -NTW disables this feature.

-P[=<file|device>] Print security report

Directs Sophos Anti-Virus to produce a report of the areas checked. Sophos Anti-Virus outputs this report to the device PRN, if the option is used as -P (not followed by =).

Alternatively, the report can be directed to a particular file or device using the option as -P=. For example

```
SWEEP -P=SEC.TXT
```

directs Sophos Anti-Virus to write its security report to the file SEC.TXT.

-PAT=<Hex> Pattern specification

Allows patterns to be specified at the command line. This may be useful to check for a particular pattern as a one-off. The pattern must be specified as a string of hexadecimal digits without any blanks as separators and can be up to 24 bytes (48 hexadecimal characters) long.

If found, such patterns are reported as ‘Command line 1’, etc.

Sophos Anti-Virus looks for patterns only when performing a full scan, specified by -F.

For example

```
SWEEP -PAT=23f78172bca918e1 -F
```

-PB Display progress bar

Enables Sophos Anti-Virus to display a progress bar.

To do this, Sophos Anti-Virus has to count all the items to be scanned before starting, which means the scan takes slightly longer. On very large network drives, this can have a significant impact on performance.

-PD Pause on discovery of a match

Causes Sophos Anti-Virus to pause whenever it discovers a matching pattern and wait for a keystroke before continuing.

-Q Quick sweep

By default, Sophos Anti-Virus performs a quick scan. -Q is only necessary if full scanning has been switched on using -F. This might have been done, for example, in a batch file or in a file specified by @file.

-RAR Scan inside .rar files

Enables Sophos Anti-Virus to scan inside .rar files.

-REC Recursive search

This option directs SWEEP to search directories below the ones specified in the command line.

For example

```
SWEEP C:\*.DLL C:\SIMULATI\*.SYM -REC
```

searches all DLL files on the disk starting from the root directory (\), as well as all SYM files from the \SIMULATI directory downwards.

-REMOVE Remove viruses on discovery

Directs Sophos Anti-Virus to delete any infected files and disable any infected boot sectors.

-RS can be used in conjunction with -REMOVE to ensure the file is positively overwritten rather than deleted.

Confirmation will be requested before any item is deleted or disabled unless -NOC is also used.

Disabling of boot sectors is done by substituting the first two bytes pointed to by the initial JMP instruction with a JMP-to-itself instruction. Note that after disabling a boot sector, the virus fragment may still be there, but the virus will be totally inactive.

For example

```
SWEEP -REMOVE
```

or

```
SWEEP -REMOVE -RS -NOC
```

-REMOVEB Disable infected boot sectors

As -REMOVE, except that infected files are not removed.

-REMOVEF Remove infected files

As -REMOVE, except that infected boot sectors are not disabled.

-RS Remove viruses by positively overwriting them

Causes Sophos Anti-Virus to remove any infected files by positively overwriting them, instead of just deleting them.

Disabling of boot sectors is not affected.

-RS has no effect unless -REMOVE or -REMOVEF is also specified.

For example

```
SWEEP -REMOVE -RS
```

❗ **Files overwritten when this option is used cannot be recovered.**

-S Silent running without displaying checked areas

By default, Sophos Anti-Virus does not display on the screen the areas it is scanning. -S is equivalent to this default mode, and is the opposite of -NS.

-SFX Scan self-extracting archives

Enables Sophos Anti-Virus to scan inside self-extracting archives. It must be used with a specific archive type. For example

```
-SFX -ZIP
```

-SS Super silent running

Prevents Sophos Anti-Virus from displaying anything (not even the copyright message) unless a virus is found.

-UUE Scan .uue files

Enables Sophos Anti-Virus to scan .uue files.

-V Version information

Causes Sophos Anti-Virus to display the Sophos Anti-Virus copyright information and version number.

-VV Extended version information

Causes Sophos Anti-Virus to display extended version information, including the following:

- version numbers of the virus data, the virus engine and the virus engine interface
- the release date
- a list of filename extensions that are scanned by default
- a table of archive file types that can be scanned
- a table of virus engine options
- a list of languages supported by Sophos Anti-Virus.

The table of archive file types and the table of virus engine options list the following:

- the name of the archive file type or engine option
- whether this is on or off
- the specific command line option to turn on scanning inside this archive file type or turn on this engine option
- the group command line option in which this option is included (e.g. -MACARC includes -APPLE, -BHEX, -MBIN and -SIT)
- the filename extensions associated with this archive file type or engine option.

You can turn *off* an engine option or scanning of an archive type by preceding the relevant option with “N” (e.g. -NACCESS turns off scanning of Microsoft Access files).

If you type

```
SWEEP -VV -ARCHIVE
```

the list of filename extensions, the table of archive file types and the table of virus engine options change to indicate what is scanned when you use -ARCHIVE.

-XML

Enables Sophos Anti-Virus to scan .xml files.

-ZIP Scan inside .zip files

Enables Sophos Anti-Virus to scan inside .zip files.

Updates

Performing a monthly update

Performing an emergency update

6 Performing a monthly update

Registered users of Sophos Anti-Virus are sent a new Sophos Anti-Virus CD in the first week of every month. Alternatively, you can download the updated version from the Sophos website. To update Sophos Anti-Virus

- **on a workstation**, follow the steps in section 1.2.
- **on a file server** for use by workstation users, see section 1.3.

7 Performing an emergency update

Whenever there is a new virus that poses a threat to your system, update Sophos Anti-Virus as soon as possible with the virus identity file (IDE) for the virus.

IDEs consist entirely of printable ASCII characters, and can be downloaded from the Sophos website (www.sophos.com/downloads/ide). They can also be emailed or faxed.

Save new IDEs to the folder from which Sophos Anti-Virus is run. Assuming that Sophos Anti-Virus was installed as described in this manual, this is the directory that contains SWEEP.EXE (by default SWEEP).

💡 To receive email notifications about IDEs and other alerts, register at www.sophos.com/virusinfo/notifications.

Troubleshooting

8 Troubleshooting

This section provides answers to some common problems that can be encountered when using Sophos Anti-Virus.

If your problem is not described in this section, refer to the Sophos website www.sophos.com which includes a support knowledgebase, virus analyses, the latest IDEs, product downloads and technical articles.

If your problem is not described on the website, contact Sophos technical support.

8.1 SWEEP runs slowly

Full sweep

By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files likely to contain a virus. However, if full scanning is enabled, Sophos Anti-Virus will run significantly slower. See also section 4.3.

No extended or expanded memory

If Sophos Anti-Virus does not find extended or expanded memory, it creates a ‘swap’ file on the hard disk or on a network drive. To increase the scanning speed, install the extended or expanded memory manager. For example, to use extended memory, insert the following line into CONFIG.SYS:

```
DEVICE=HIMEM.SYS
```

and copy HIMEM.SYS onto the floppy. When the computer is next booted, extended memory will be available to Sophos Anti-Virus.

If the computer does not have extended or expanded memory, the location of the swap file can be specified by setting the TMP environment variable.

For example, type

```
SET TMP=C:
```

Checking all files or all sectors

By default, Sophos Anti-Virus only scans files defined as executables. If Sophos Anti-Virus is scanning all files, it will take longer than if only executable files are being scanned. All files can be scanned using -ALL or by including a descriptor such as

```
>\*.*
```

in the SWEEP.ARE file (see section 4.8).

Network drives

Some network drives will be much larger than a local hard disk, and so will take significantly longer to scan. Most network interfaces provide much slower access than a local hard disk, which can reduce speed further still.

8.2 Out of memory

Apart from the conventional memory, Sophos Anti-Virus also uses extended memory, expanded memory or disk space during its execution. If it runs out of memory, it produces a message to that effect.

Non-conventional memory requirement is currently about 340KB, but this may increase in the future.

8.3 Network Error: file in use

If a network file is already open when Sophos Anti-Virus tries to examine it, a message similar to the following is displayed and the execution of Sophos Anti-Virus is interrupted:

```
Network Error: file in use during OPEN A FILE.  File = F:\ARCHLOG\00000041.REC
Abort, Retry?
```

If a file is to be accessible to several processes at the same time, it must be marked as shareable using the NetWare utility FILER.

Alternatively, Sophos Anti-Virus can be instructed to ignore these messages and continue execution using -NI:

```
SWEEP -NI
```

The above error usually occurs when -ALL is used.

8.4 Could not open file F:\PUBLIC\SWEEP.EXE

This error message is displayed if SWEEP is run from a NetWare file server after being set as an execute-only attribute.

To remedy the problem, delete SWEEP.EXE on the network and reinstall it from the distribution disk.

8.5 Virus fragment reported

A virus fragment report indicates that part of a file matches part of a virus. There are three possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active. If you suspect that this is the case, please send Sophos a sample and a description.

Corrupted virus

Many viruses contain bugs in their replication routines so that they sometimes infect target files incorrectly.

A portion of the virus body (possibly a substantial part) may appear within the host file, but in such a way that it will never be actuated. In this case, Sophos Anti-Virus reports a virus fragment rather than a virus. A corrupted virus cannot normally spread.

If a virus fragment is reported, contact Sophos technical support for advice.

Database containing a virus

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file. Contact Sophos technical support for advice.

Appendices

Appendix 1 Scheduling Sophos Anti-Virus

This section describes how to schedule scans using the AT utility.

The AT utility is only available to users with DOS file (server) site licences.

Scheduling means you can carry out scanning at quiet times, such as overnight.

Appendix 1.1 Setting up a schedule in AT.INI

For an example AT.INI file, go straight to appendix 1.4.

The Sophos Anti-Virus schedule and commands are listed in the AT.INI file.

The AT.INI file must reside in the current directory of the current drive when AT.EXE is run. An alternative path and file can be specified in the command line when AT.EXE is started.

AT.INI is a text file containing two types of entries:

- **Action entries** specify what should happen.
- **Time entries** specify when it should happen. Time entries always specify the timing of the preceding Action entries.

Action entries start in the first column, while Time entries start with one or more Spaces or Tabs.

Example AT.INI file

```
ECHO Meeting
  9:30 Mon,Thu
ECHO Lunch
  12:30 Mon,Tue,Wed,Thu,Fri
```

This would display ‘Meeting’ at 09:30 every Monday and Thursday and ‘Lunch’ every week day at 12:30.

Appendix 1.1.1 Action entries in the AT.INI file

Action entries can start any DOS command, program or a batch file, and are passed on to the system exactly as entered in AT.INI.

It is possible to specify more than one Action entry to be associated with a Time entry. For example

```
ECHO Here is a DIR at 09:00
DIR C:
  09:00 Mon
```

would cause the display of the text and the execution of the DIR command at 9:00 a.m. every Monday.

No command executed by the AT command should require keyboard input since no further scheduled commands will be executed until the command terminates. When launching Sophos Anti-Virus, use the -NK command line option, which prevents it from asking for user input.

For example

```
SWEEP F: -NK -P=SWEEP.LOG
  07:00
  19:00
```

would start Sophos Anti-Virus at 7:00 and 19:00 every day, storing the output in the SWEEP.LOG file.

Appendix 1.1.2 Time entries in the AT.INI file

Time entries refer to the preceding Action entries. A time entry must start with a Tab and consists of an (optional) time followed by an optional day or date.

Time is specified in 24-hour format and wildcard characters (?) are allowed. For example

```
ECHO Hello!
  7:00 Mon
  12:00 Mon,Tue,Wed,Thu,Fri
  ??:30
ECHO It's my birthday today!
  22/4
ECHO I am 30 today!
  22/4/98
```

would display ‘Hello!’ at 7:00 on Monday, at 12:00 on all workdays and at 30 minutes past each hour. It would also display ‘It's my birthday today!’

every 22nd April, while on 22nd April 1998 it would (also) display ‘I am 30 today’.

If a ‘+’ follows the time, it means ‘at that time or later’. For example:

```
ECHO Dinner
  19:00+
```

would display ‘Dinner’ when AT is executed at any time between 19:00 and 23:59.

Time entries can also contain a date, which may contain wildcards. For example:

```
SEND "It's the 5th!" TO EVERYBODY
  0:00 5/?/98
```

would execute the command ‘SEND’ at 0:00 on the 5th of every month during 1998.

Dates are specified in European style, i.e. day, month, year. Months can be spelled out, e.g. January, but the first 3 characters must be given.

Appendix 1.1.3 Comments in the AT.INI file

Any entry can contain comments after ‘;’ which are ignored. For example

```
; This is a comment
ECHO Good evening! ; a greeting
  19:00
```

Appendix 1.2 Starting the scheduler

AT.EXE must be running in order to execute scheduled commands. This is normally accomplished by running it as a background task within Windows or on a soft Windows workstation on the server.

To invoke AT, type ‘AT’ at the DOS command line. For example

```
C:> AT
```

AT command will read the AT.INI file at startup as well as whenever AT.INI is modified. This allows you to edit AT.INI in one Window while AT is running in the second one. When the new AT.INI is saved, AT will reread it and modify the scheduled events accordingly.

AT checks the syntax of AT.INI whenever it is read. If AT.INI is edited, it is possible to check that the syntax is right: simply save the file and run AT. If AT does not complain, the syntax is correct.

Appendix 1.3 AT command line options

AT command line options can be specified in the command line. For example

```
AT -SS MYFILE.INI
```

The options are as follows.

-NOW Execute all events now

When this is used, AT will execute all events from AT.INI file immediately. This option is used for testing.

-NP No pause

By default, the AT command waits until a scheduled event occurs. If the user wishes to check if any events are scheduled and not wait until a scheduled event occurs, the -NP option is used.

For example, insert the command

```
AT -NP
```

in AUTOEXEC.BAT and edit the AT.INI file in the root directory to contain

```
ECHO Happy Christmas!
  25/12
```

AT will print out the message on 25th December and continue to execute the rest of the commands in AUTOEXEC.BAT.

-SS Super Silent mode

If this command line option is used, AT will not display anything on the screen until a scheduled event occurs.

-? Display command line options

This causes AT to display command line options.

<filename> Alternative to AT.INI

It is possible to specify an alternative file which will be used instead of AT.INI by placing it in the command line. For example:

```
AT MYAT.INI
```

Appendix 1.4 Example AT.INI file

In this example Sophos Anti-Virus is set up to scan network drives F: and G: automatically every day at 07:00, 13:00 and 19:00 plus 22:00 on Fridays.

This is done within Windows (the Windows computer must be left on 24 hours a day).

The report will be sent to F:\REP\SWEEP.LOG and, if Sophos Anti-Virus discovers a virus, the SUPERVISOR will be paged (providing the system supports the PAGE command).

SWEEP.EXE and AT.EXE are assumed to be in the F:\SWEEP directory.

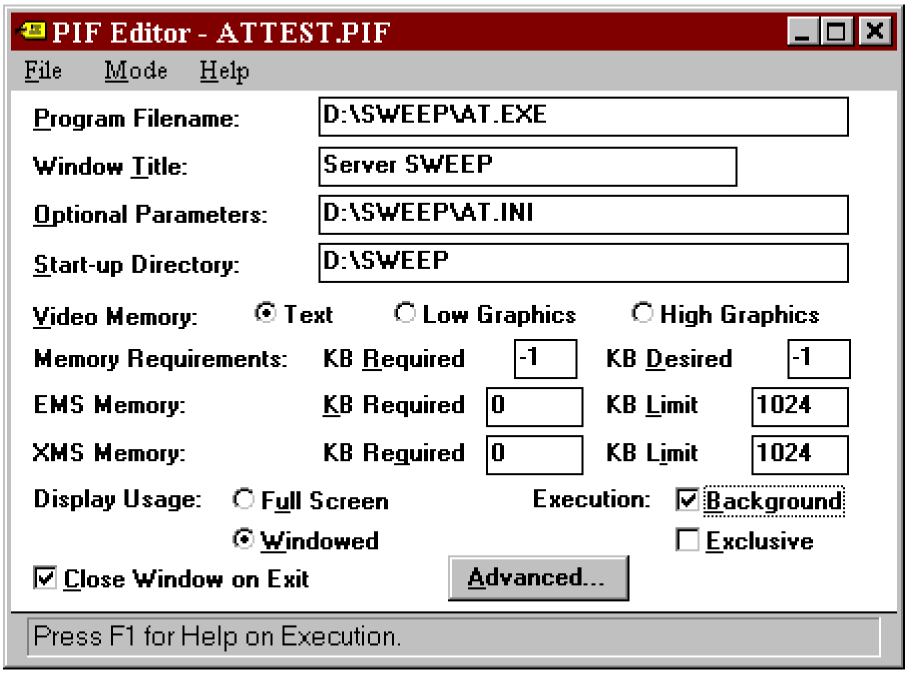
1. Using a text editor, add the following text to F:\AT.INI:

```
F:\SWEEP\MYSCAN.BAT
  07:00
  13:00
  19:00
  22:00 Fri
```

2. Create and edit a file F:\SWEEP\MYSCAN.BAT that contains the following commands:

```
SWEEP F: G: -NK -P=F:\REP\SWEEP.LOG
IF ERRORLEVEL 3 GOTO VIRUS
GOTO END
:VIRUS
PAGE SUPERVISOR "Virus alert!"
:END
```

3. From within Windows use the PIF editor to create the file AT.PIF with the following specifications:



Program Filename: D:\SWEEP\AT.EXE

Window Title: Server SWEEP

Optional Parameters: D:\SWEEP\AT.INI

Start-up Directory: D:\SWEEP

Video Memory: ● Text ○ Low Graphics ○ High Graphics

Memory Requirements: KB Required -1 KB Desired -1

EMS Memory: KB Required 0 KB Limit 1024

XMS Memory: KB Required 0 KB Limit 1024

Display Usage: ○ Full Screen ● Windowed

Execution: ☑ Background □ Exclusive

☑ Close Window on Exit

Press F1 for Help on Execution.

4. Save the file.

5. Open the StartUp group in Windows.

6. Using File manager pick up AT.PIF and drag it to the StartUp group.

7. Test the correct functioning of AT by double-clicking it. This should start the AT command, and the DOS box will show the current time and date.

   When the next scheduled event is due, AT will load Sophos Anti-Virus and execute it.

   Since the icon has been placed in the StartUp group, the scheduled process will be restarted automatically whenever Windows is started.

Glossary and index

Glossary

ASCII

American Standard Code for Information Interchange; the standard system for representing letters and symbols. Each letter or symbol is assigned a unique number between 0 and 127.

BAT

The extension given to the names of batch files in MS-DOS. A batch file contains a series of MS-DOS commands, which can be executed by using the name of the file as a command. AUTOEXEC.BAT is a special batch file which is executed whenever a computer is switched on, and can be used to configure the computer to a user’s requirements.

Booting

The process carried out when a computer is first switched on or reset, where the operating system software is loaded from disk.

Boot sector

The part of the operating system which is first read into memory when a computer is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.

Boot sector virus

A type of virus that subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Checksum

A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered.

COM

The extension given to a type of executable file in MS-DOS. A COM file is similar to an EXE file, but can only contain up to 64K of code and data. In operating systems other than DOS, COM can have a different significance.

Companion virus

A virus which infects EXE files by creating a COM file with the same name which contains the virus code. It exploits the DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.

Conventional memory

The bytes of PC memory addressable by the 8086 instruction set.

DOS boot sector

The boot sector which loads the BIOS and DOS into RAM and starts their execution. Common point of attack by boot sector viruses.

EXE

The extension given to executable files in MS-DOS. These are similar to COM files, but can contain more than 64KB of code and data.

Expanded memory

Memory which conforms to the industry standard specification EMS (Expanded Memory Specification), and enables the CPU to access more than 640K of memory.

Extended memory

Memory above 1 MB in a 80286 (or above) computer.

False negative

An existent event reported as non-existent (e.g. the absence of a virus when the virus is present)

False positive

A non-existent event reported as existent (e.g. the presence of a virus when no virus is present)

FAT

File Allocation Table; a term used by the MS-DOS operating system (and others) to describe the part of a disk which contains information describing the physical location on the disk of the chains of clusters forming the files stored on that disk.

Hexadecimal

A system of counting using number base 16. The numbers 10 to 15 are represented by the characters A through F respectively. Hexadecimal is often abbreviated to Hex. Each Hex digit is equivalent to four bits (half a byte) of information.

IDE (Virus Identity File)
A type of file that contains the data Sophos Anti-Virus needs to enable it to detect and disinfect a specific virus. IDEs are issued in between monthly updates to keep Sophos Anti-Virus up to date with the very latest viruses.

Interrupt
A mechanism by which a process can attract the immediate attention of the CPU, usually in order to serve an urgent request from an external device.

Link virus
A virus which subverts directory entries to point to the virus code.

Macro virus
A type of virus which uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.

Master boot sector
The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the computer is booted. It contains the partition table as well as the code to load and execute the boot sector of the active partition. Common point of attack by boot sector viruses.

Memory-resident virus
A virus that stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only when an infected application is running.

Multipartite virus
A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

Parasitic virus
A virus which attaches itself to another computer program, and is activated when that program is executed. A parasitic virus can attach itself to either the beginning or the end of a program, or it can overwrite part of the program.

Partition table

A 64-bit table found inside the master boot sector on hard disks which contains information about the starting and ending of up to four partitions on the hard disk. The partition table also contains information on the type of the partition (e.g. DOS partition, Unix partition etc).

Polymorphic virus

A self-modifying encrypting virus.

Primary DOS partition

A portion of the hard disk assigned exclusively to DOS. It is usually the bootable partition for DOS.

Stealth virus

A virus which hides its presence from the user and anti-virus programs, usually by trapping interrupt services.

SYS

The extension given to system file names in MS-DOS. An example is the file CONFIG.SYS which sets up various configuration parameters for the operating system on power-up.

Trojan horse

A computer program which carries out hidden and harmful functions. Generally Trojan horses trick the user into running them by claiming to have legitimate functionality. Backdoor Trojans enable other users to take control of your computer over the internet.

UNC

Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.

VDL

Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically.

Virus pattern

A sequence of bytes extracted from a virus and used for virus recognition.

Index